Sérvulo & Associados | Sociedade de Advogados, SP, RL

Maio 2020

Update

Privacidade e Proteção de Dados Pessoais

COVID-19

COVID-19: Aplicações de rastreamento de contactos e proteção de dados

Mariana Teles | mpt@servulo.com

O desenvolvimento de aplicações informáticas de rastreamento da proximidade entre pessoas com o objetivo de evitar a propagação da pandemia de COVID-19 tem sido tema de discussão na atualidade, por causa dos riscos que podem comportar para a privacidade das pessoas, particularmente numa fase em que se tem projetado a mitigação de medidas de confinamento, como sucede em Portugal.

Ciente desses riscos, o Comité Europeu para a Proteção de Dados[1] (CEPD) adotou, no passado dia 21 de abril de 2020, um conjunto de diretrizes gerais para todos aqueles que se propõem desenvolver e pôr em funcionamento tais aplicações nos Estados-Membros da União Europeia e do Espaço Económico Europeu, com o propósito de que a conceção e o desenvolvimento dessas aplicações se façam com respeito pelas leis de proteção de dados pessoais, principalmente o Regulamento Geral sobre a Proteção de Dados.

Damos nota, em linhas muito breves, das características destas aplicações e dos principais requisitos de proteção de privacidade que o CEPD refere.

O que são aplicações de rastreamento de contactos?

Em termos muito simples, aplicações de rastreamento de contactos são programas informáticos (software)desenvolvidos e criados especificamente para telemóveis ou equipamentos móveis semelhantes (computadores, tablets, etc.), que permitem trocar informações com outros dispositivos do mesmo género que estejam próximos. No caso, a função principal da aplicação é detetar a proximidade de dispositivos de utilizadores que sejam portadores do vírus SARS-Cov-2.

Qual a sua finalidade?

O propósito destas aplicações consiste em alertar os seus utilizadores de que podem ter sido expostos ao vírus em razão da distância e da duração da proximidade (ou do contacto) que tiveram com um utilizador portador do vírus e apresentar-lhes recomendações.

Rua Garrett, 64
1200-204 Lisboa – Portugal
T. +351 210 933 000

geral@servulo.com
www.servulo.com

Estas aplicações não podem ser utilizadas para outros fins. Por exemplo, não podem ser utilizadas para controlar o cumprimento da quarentena ou das medidas de confinamento e de distanciamento social, nem para extrair conclusões sobre as localizações dos seus utilizadores.

São obrigatórias?

A utilização das aplicações deve ser sempre voluntária, o que significa que apenas devem ser instaladas e utilizadas pelas pessoas que o quiserem fazer. Aqueles que as não utilizarem ou não possam utilizar não podem ser afetados nos seus direitos. Por outro lado, as aplicações também dependem da vontade do utilizador que for portador do vírus em comunicar essa informação, que aliás deve partir de um consentimento específico do próprio e deve ser confirmada por laboratórios de testes ou por profissionais de saúde.

Existem restrições à recolha de dados?

As aplicações não devem recolher dados para além dos estritamente necessários para efeitos de rastreamento de contactos. Por exemplo, considera-se que não são necessários dados de estado civil, identificadores de comunicação, referências de diretórios de equipamentos, mensagens, registos de chamadas, dados de localização, identificadores de dispositivos e ainda dados relativos à saúde para além dos estritamente necessários.

No que diz respeito aos dados de localização, apenas excecionalmente podem ser tratados com a única finalidade de permitir que as aplicações sejam interoperáveis, isto é, que interajam com aplicações semelhantes existentes noutros países.

Além disso, as informações recolhidas devem permanecer no equipamento terminal do utilizador e apenas as informações relevantes devem ser recolhidas quando tal for absolutamente necessário.

Mais, os utilizadores devem ser informados de todos os dados pessoais que serão recolhidos e essa recolha apenas pode ocorrer com o consentimento do utilizador.

Que especificidades devem ter os dados a transmitir?

Os dados a transmitir entre os dispositivos dos utilizadores, bem como entre esses dispositivos e computadores ou programas servidores centrais que possam apoiar o funcionamento da aplicação, se os houver, não podem incluir dados de identificação dos dispositivos que não sejam dados únicos, pseudonimizados, gerados pela própria aplicação. Estes dados devem ser renovados regularmente, de forma a restringir os riscos de identificação dos utilizadores a que dizem respeito, de rastreamento dos seus movimentos ou da sua ligação a outros utilizadores.

As aplicações podem automaticamente realizar o diagnóstico ou dar conselhos médicos aos utilizadores?

Uma das medidas recomendadas para estas aplicações consiste na elaboração de um sistema que permita confirmar que o utilizador que reportou ter um teste positivo de SARS-CoV-2 está realmente infetado. Pretende-se que um profissional de saúde intervenha e confirme esse estado de saúde do utilizador. Se a confirmação não for obtida de forma segura, esse dado não pode ser utilizado.

Rua Garrett, 64
1200-204 Lisboa – Portugal
T. +351 210 933 000
geral@servulo.com
www.servulo.com

As aplicações não podem substituir o contacto realizado por profissionais de saúde pública qualificados, devendo existir sempre uma estrita supervisão por estes profissionais, de forma a limitar a ocorrência de falsos negativos e falsos positivos.

Por outro lado, as aplicações podem prestar recomendações aos utilizadores identificados como potencialmente expostos ao vírus, mas esta tarefa de aconselhamento não pode basear-se apenas num processamento automatizado, sendo obrigatória a intervenção humana.

As aplicações podem permitir a identificação dos utilizadores?

As aplicações não podem permitir que os utilizadores sejam diretamente identificados quando utilizam a aplicação. Além disso, não podem permitir rastrear os movimentos nem sequer deduzir informações de outros utilizadores, especialmente se são ou não portadores do vírus. A aplicação só deve revelar a cada utilizador se foi exposto ao vírus e, se possível, o número de horas e datas de exposição, sem revelar informações sobre outros utilizadores.

Como podem os utilizadores da aplicação exercer os seus direitos sobre os seus dados pessoais?

A própria aplicação deve proporcionar ao utilizador meios de exercer os seus direitos referentes aos seus dados pessoais, em particular os direitos prescritos no Regulamento Geral sobre a Proteção de Dados.

Para além disto, a aplicação deve estabelecer de forma clara e explicada aos utilizadores quais os papéis e responsabilidades dos diferentes atores que contribuíram para a implementação da aplicação, em especial quem é ou quem são os responsáveis pelo tratamento de dados da aplicação.

Por quanto tempo podem ser mantidos os dados recolhidos pelas aplicações? Qual a duração das aplicações?

O Comité não define prazos. Adianta apenas que a conservação dos dados deve ser limitada pelas necessidades e pela relevância médica dos dados (por exemplo o período de incubação) e que os dados pessoais devem ser mantidos apenas durante a crise. Depois disso devem ser apagados ou anonimizados.

Contudo, no fim da situação excecional de pandemia, o mais tardar, as autoridades públicas competentes devem instituir um procedimento para fazer cessar o funcionamento da aplicação, por exemplo por meio da desativação da aplicação, de instruções para que os utilizadores a desinstalem ou de desinstalação automática, e eliminar todos os dados recolhidos de todas as bases de dados. Por outro lado, a utilização das aplicações deve ser possível apenas até que as técnicas de rastreamento de contacto através de intervenção humana consigam gerir a quantidade de novas infeções.

Aqui chegados, importa notar que estas diretrizes não são (nem podiam ser) exaustivas, o que significa que o seu cumprimento pode não ser suficiente para assegurar a conformidade com o quadro legal da proteção de dados. Cada aplicação deve ser avaliada em concreto, podendo estar sujeita a requisitos adicionais. Por outro lado, outras soluções tecnológicas podem ser implementadas, diferentes daquelas

Rua Garrett, 64
1200-204 Lisboa – Portugal
T. +351 210 933 000
geral@servulo.com
www.servulo.com

que foram consideradas pelo Comité, desde que lícitas. Ou seja, é necessário aguardar para conhecer as aplicações concretas implementadas e fazer essa avaliação.

---

[1] O Comité Europeu para a Proteção de Dados é um organismo da União Europeia que tem por missão assegurar a aplicação coerente do Regulamento Geral sobre a Proteção de Dados na U.E., sendo composto pelo diretor de uma autoridade pública de cada Estado-Membro com competência para fiscalizar as leis de proteção de dados pessoais e da Autoridade Europeia para a Proteção de Dados, ou pelos respetivos representantes.

Rua Garrett, 64
1200-204 Lisboa – Portugal
T. +351 210 933 000

geral@servulo.com
www.servulo.com